A Simple Algorithm for Local Conversion of Pure States

Jens G Jensen and Rüdiger Schack
Dept. of Mathematics, Royal Holloway, University of London
Egham, Surrey TW20 0EX, UK

June 13, 2000

Abstract

We describe an algorithm for converting one bipartite quantum state into another using only local operations and classical communication, which is much simpler than the original algorithm given by Nielsen [Phys. Rev. Lett. **83**, 436 (1999)]. Our algorithm uses only a single measurement by one of the parties, followed by local unitary operations which are permutations in the local Schmidt bases.

1 Introduction

Consider the case where two parties, Alice and Bob, share an entangled state of two N-level particles. M. A. Nielsen introduced in [N] an algorithm for converting one such pure bipartite state into another using only local operations and classical communication. He gave an explicit condition for when such a conversion is possible: We write the first state in Schmidt form

$$|\phi\rangle = \sum_{i=1}^{N} \sqrt{\alpha^i}|i\rangle \otimes |i\rangle, \tag{1}$$

where the α^i are non-negative real numbers satisfying $\sum_i \alpha^i = 1$, and similarly for the target state

$$|\psi\rangle = \sum_{i=1}^{N} \sqrt{\beta^i}|i\rangle \otimes |i\rangle. \tag{2}$$

Then $|\phi\rangle$ may be converted to $|\psi\rangle$ iff the vector (β^i) *majorizes* (α^i), i.e.,

$$\forall k: \quad \sum_{i=1}^{k} {}^{\downarrow}\beta^i \geq \sum_{i=1}^{k} {}^{\downarrow}\alpha^i \tag{3}$$

with equality for $k = N$; here ${}^{\downarrow}\beta^i$ are the β^i arranged in descending order, and similarly for the ${}^{\downarrow}\alpha^i$. This is again equivalent (theorem II.1.10 of [Bh]) to the existence of a doubly stochastic matrix D such that $\alpha = D\beta$ (a doubly stochastic matrix has non-negative real entries, and all its rows and columns sum to one).

Nielsen's algorithm uses several rounds of individual measurements and classical communication. Although it is known that such a sequence of operations can be replaced by one involving only a single measurement [LP], the proof of this is non-constructive and not easily applied to Nielsen's algorithm. Our simpler algorithm may be useful for practical applications and for the analysis of local pure-state conversion in quantum cryptography [B, JS].

2 Example

In this section we illustrate how the algorithm works by an example. We consider the case $\beta^T = (\beta^i)^T = (3/5, 3/10, 1/10)$ and $\alpha^T = (\alpha^i)^T = (2/5, 1/4, 7/20)$ (for typographic reasons, we write the transpose of the column

vectors); note that α is not sorted: as we shall see, this doesn't matter. We check that $\beta \succ \alpha$. Using the algorithm from (the proof of) theorem II.1.10 in [Bh], we find a doubly stochastic matrix that maps β to α:

$$\begin{pmatrix} 1/3 & 2/3 & 0 \\ 1/6 & 1/3 & 1/2 \\ 1/2 & 0 & 1/2 \end{pmatrix} \begin{pmatrix} 3/5 \\ 3/10 \\ 1/10 \end{pmatrix} = \begin{pmatrix} 2/5 \\ 1/4 \\ 7/20 \end{pmatrix} \tag{4}$$

From this matrix we now derive the set of unitary transformations, which turn out to be permutations. We start by finding a set of *non-zero* entries with no two entries in the same row or in the same column, i.e., corresponding to some permutation matrix. We first choose positions $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, corresponding to the permutation (12). The smallest entry in the doubly stochastic matrix in these positions is 1/6, so we subtract 1/6 times the permutation matrix. Then we get

$$\begin{pmatrix} 1/3 & 1/2 & 0 \\ 0 & 1/3 & 1/2 \\ 1/2 & 0 & 1/3 \end{pmatrix} \tag{5}$$

Again we look for a set of non-zero entries with no two in the same row or column; let's pick the identity matrix this time. The smallest entry on the main diagonal of (5) is 1/3, so we subtract 1/3 times the identity matrix, and finally we are left with 1/2 times a permutation matrix corresponding to the permutation (132).

Using the above decomposition, we can now rewrite (4) as

$$\begin{pmatrix} 3/10 & 3/5 & 3/10 \\ 3/5 & 3/10 & 1/10 \\ 1/10 & 1/10 & 3/5 \end{pmatrix} \begin{pmatrix} 1/6 \\ 1/3 \\ 1/2 \end{pmatrix} = \begin{pmatrix} 2/5 \\ 1/4 \\ 7/20 \end{pmatrix} \tag{6}$$

We may imagine that the columns in the matrix are indexed by the permutations we found above, i.e., (12), (), and (132), respectively. The entries of column σ are then β permuted by σ^{-1}; we permute the vector by shuffling the components: $(\beta^1, \beta^2, \beta^3).(123) = (\beta^2, \beta^3, \beta^1)$ (this corresponds to the last row because $(132)^{-1} = (123)$). Thus, in the column corresponding to σ, the ith row has the entry $\beta^{\sigma^{-1}(i)}$. The LHS vector in (6) is (p^σ), where the p^σ is the weight corresponding to σ that we found above when decomposing the doubly stochastic matrix. The RHS vector is, of course, α.

Now we need to find the POVM. To do this, we find three diagonal matrices A_σ, each defined by taking column σ and dividing the ith entry (in the ith row) with α^i, and multiplying with p^σ. Thus

$$A_{(12)} = \tfrac{1}{6}\mathrm{diag}(\tfrac{3/10}{2/5}, \tfrac{3/5}{1/4}, \tfrac{1/10}{7/20}) = \mathrm{diag}(1/8, 2/5, 1/21) \tag{7}$$

$$A_{()} = \tfrac{1}{3}\mathrm{diag}(\tfrac{3/5}{2/5}, \tfrac{3/10}{1/4}, \tfrac{1/10}{7/20}) = \mathrm{diag}(1/2, 2/5, 2/21) \tag{8}$$

$$A_{(123)} = \tfrac{1}{2}\mathrm{diag}(\tfrac{3/10}{2/5}, \tfrac{1/10}{1/4}, \tfrac{3/5}{7/20}) = \mathrm{diag}(3/8, 1/5, 6/7) \tag{9}$$

We observe that each A_σ is a positive matrix, and that the sum of the A_σ is the identity matrix. The A_σ thus define a POVM. All we now need to see is what happens when the corresponding operations are applied to the state described by α.

The POVM is performed locally by one of the parties, say Alice. In our example, the post-measurement state corresponding to the outcome σ is a pure state with Schmidt coefficients obtained by normalizing the vector $A_\sigma\alpha$:

- (12): $(1/20, 1/10, 1/60) \rightsquigarrow (3/10, 3/5, 1/10)$
- (): $(1/5, 1/10, 1/30) \rightsquigarrow (3/5, 3/10, 1/10)$
- (123): $(3/20, 1/20, 3/10) \rightsquigarrow (3/10, 1/10, 3/5)$

where the $\rightsquigarrow$ indicates the normalization. The post-measurement states are thus given by the columns of the matrix in equation (6). To reach the target state, Alice permutes the bases according to the permutation σ, and she communicates σ to Bob who then performs the same permutation on his basis.

3 Formal Description and Proof

3.1 Description of the algorithm

Find the doubly stochastic matrix

Given vectors of Schmidt coefficients α and β such that $\beta \succ \alpha$, we first use the algorithm of [Bh], II.1.10, to find a doubly stochastic matrix D such that $\alpha = D\beta$.

Decompose the doubly stochastic matrix

The Birkhoff-von Neumann theorem ([Bh], chapter 2) states that we can find permutations $\sigma \in \Sigma \subseteq \mathfrak{S}_N$ and positive numbers p^σ such that

$$D = \sum_{\sigma \in \Sigma} p^\sigma P_\sigma \tag{10}$$

where P_σ is the permutation matrix associated to σ, i.e., it maps the fundamental vector e_i (with a one in the ith place and zeros otherwise) to $e_{\sigma(i)}$.

To explicitly find the decomposition of the density matrix, we may use that many of the proofs of the Birkhoff-von Neumann theorem are constructive. The approach we sketch here is similar to the proof in [P].

It will be useful to define an *arrangement* (or *diagonal*) of a $n \times n$ matrix $M = (m^i_j)$ as a set of entries $\{m^{\sigma(i)}_i\}$ for some permutation $\sigma \in \mathfrak{S}_n$, i.e., where no two entries are taken from the same row or the same column. It follows from the König-Frobenius theorem ([Bh], chapter 2) that any doubly stochastic matrix has an arrangement with all entries non-zero.

There is a polynomial-time algorithm for finding such arrangements in a matrix: Consider the matrix $\tilde{D}$ which is D with each non-zero entry replaced by 1. Let $R = \{r_1, \ldots, r_n\}$ be the set of row indices of $\tilde{D}$ and $C = \{c_1, \ldots, c_n\}$ the set of column indices. Then $\tilde{D}$ defines a balanced bipartite graph G with vertices $R \cup C$ (disjoint union): we have an edge from r_i to c_j iff $\tilde{D}^i_j = 1$. By the König-Frobenius theorem, G has no isolated nodes. We can thus easily find a perfect matching in the graph; there are polynomial-time algorithms for doing this, see e.g., chapter 3, section 3 of [P]. A perfect matching defines a unique permutation $\sigma \in \mathfrak{S}_n$ through its edges $r_{\sigma(i)} \leftrightarrow c_i$, $i = 1, \ldots, n$. It is easy to see that the matching also defines an arrangement of D with all entries non-zero.

Constructing the POVM

Now we assume that we have the decomposition (10). Hence

$$\forall i: \quad \sum_\sigma \beta^{\sigma^{-1}(i)} p^\sigma = \alpha^i \tag{11}$$

Indeed, $\alpha^i = (D\beta)^i = [(\sum_\sigma p^\sigma P_\sigma)\beta]^i = \sum_\sigma p^\sigma \beta^{\sigma^{-1}(i)}$.

Next, we define matrices

$$A_\sigma = p^\sigma \mathrm{diag}_i\left(\frac{\beta^{\sigma^{-1}(i)}}{\alpha^i}\right) \tag{12}$$

where $\mathrm{diag}_i(f(i))$ denotes a diagonal matrix whose (i,i) entry is $f(i)$.

The $\{A_\sigma \mid \sigma \in \Sigma\}$ define a POVM, since each A_σ is a positive matrix, and

$$\begin{aligned} \sum_\sigma A_\sigma &= \sum_\sigma p^\sigma \mathrm{diag}_i\left(\frac{\beta^{\sigma^{-1}(i)}}{\alpha^i}\right) \\ &= \mathrm{diag}_i\left(\frac{1}{\alpha^i}\sum_\sigma p^\sigma \beta^{\sigma^{-1}(i)}\right) \\ &= \mathrm{diag}_i 1 \end{aligned}$$

Furthermore,

$$\mathrm{tr}(A_\sigma \mathrm{diag}_i(\alpha^i)) = p^\sigma \tag{13}$$

so that p^σ is the probability of outcome σ.

The measurement

Now we turn to the measurement itself. When Alice performs the measurement on her side, we need only consider her reduced density matrix, ρ, which has eigenvalues α^i. We choose the operations corresponding to

the POVM A_σ such that, if the outcome of the measurement is σ, then the reduced density matrix after the measurement is

$$\rho_\sigma = \frac{1}{p^\sigma}\sqrt{A_\sigma}\rho\sqrt{A_\sigma} = \frac{1}{p^\sigma}A_\sigma\rho. \tag{14}$$

The eigenvalues of ρ_σ are $\beta^{\sigma^{-1}(i)}$, $i = 1, \ldots, N$, which sum to one. Alice then performs the permutation σ on her side, and communicates σ to Bob so that he can do the same: since $\sum_i \beta^{\sigma^{-1}(i)}|i\rangle \otimes |i\rangle = \sum_i \beta^i |\sigma(i)\rangle \otimes |\sigma(i)\rangle$, the operation should map $|\sigma(i)\rangle$ to $|i\rangle$ for all i. After the unitary operations, the particles are in the pure state $|\psi\rangle$ (2) with Schmidt coefficients β^i.

3.2 The converse

We now turn to the converse: given α and β and a POVM $\{A_\sigma \mid \sigma \in \Sigma\}$ with $\Sigma \subseteq \mathfrak{S}_n$ such that for all $\sigma \in \Sigma$,

$$(A_\sigma \alpha).\sigma = p^\sigma \beta, \tag{15}$$

for some positive constants p^σ, we show that $\beta \succ \alpha$ (of course, this also follows directly from Nielsen's theorem [N]). We assume that each A_σ is given by a diagonal matrix.

Define a matrix $\Gamma = (\gamma^i_j)$ by

$$\gamma^i_j = \sum_{\{\sigma \mid \sigma(j)=i\}} p^\sigma \tag{16}$$

Then we have

$$\begin{aligned}
\forall j: \quad \sum_i \gamma^i_j &= \sum_i \sum_{\{\sigma \mid \sigma(j)=i\}} p^\sigma \\
&= \sum_{\sigma \in \Sigma} p^\sigma = 1\,; \\
\forall i: \quad \sum_j \gamma^i_j &= \sum_j \sum_{\{\sigma \mid \sigma(j)=i\}} p^\sigma \\
&= \sum_{\sigma \in \Sigma} p^\sigma = 1\,,
\end{aligned}$$

so Γ is doubly stochastic. Now equation (15) implies $A_\sigma \alpha = p^\sigma \beta.(\sigma^{-1})$, which again implies that A_σ must be of the form (12). Finally,

$$\begin{aligned}
\forall i: \quad (\Gamma\beta)^i &= \sum_j \gamma^i_j \beta^j \\
&= \sum_j \sum_{\{\sigma \mid \sigma(j)=i\}} p^\sigma \beta^{\sigma^{-1}(i)} \\
&= \sum_{\sigma \in \Sigma} p^\sigma \beta^{\sigma^{-1}(i)} \\
&= \alpha^i. \qquad (17)
\end{aligned}$$

Thus $\Gamma\beta = \alpha$, which means that $\beta \succ \alpha$.

4 Acknowledgment

This work was motivated by a discussion in the Quantum Dynamics group at Royal Holloway between N. Lütkenhaus and the authors. This work is supported by the UK Engineering and Physical Sciences Research Council (EPSRC).

References

[B] Barnum, H.: Quantum secure identification using entanglement and catalysis, *LANL preprint quant-ph/9910072.*

[Bh] Bhatia, R.: *Matrix Analysis*, Graduate Texts in Mathematics 169, Springer, New York, 1997.

[JS] Jensen, J. G., Schack, R.: Quantum authentication and key distribution using catalysis, *LANL preprint quant-ph/0003104.*

[LP] Lo, H.-K., Popescu, S.: Concentrating entanglement by local actions—beyond mean values, *LANL preprint quant-ph/9707038v2.*

[N] Nielsen, M. A.: Conditions for a class of entanglement transformations, *Phys. Rev. Lett.* **83**(2), 1999, pp. 436–439.

[P] Pulleyblank, W. R.: Matchings and extensions, chapter 3 in vol. 1 of Graham, Grötschel, Lovász: *Handbook of Combinatorics*, MIT Press/North Holland, 1996.